IGF 2023 DC-IoT Progressing Global Good Practice for the Internet of Things

The session considered IoT governance from various perspectives. To understand baseline IoT evolution, associated challenges, opportunities and responses, the IoT could best be understood as an internet of data, devices, systems or functions. For simplicity, we can call these “Internets of X” (IoX). Each perspective brings its understanding of what is possible, desirable or undesirable and tools and processes needed for governance.

Each approach must be considered in its own terms, but they start from a common base of experience and must ultimately come together to provide good governance. This leads to the need for an ecosystem comprising of stakeholders such as technical experts, governments, service providers, manufacturers, users, standards bodies, military vs civilian organisations, etc., varying in global and regional perspectives.

One immediate consequence is that IoT governance must respect a range of perspectives. Our fundamental principles are unlikely to be universal, especially when applied to specific IoT contexts. By analogy with the sensors and actuators of the IoT itself, governance needs to ‘sense’ the interests and perspectives of all significantly affected parties and somehow balance them to inform decisions at various levels. In other words, it requires *multistakeholderism*. It is not that specific expert groups (e.g., engineers) are insensitive to the needs of others (e.g., end users) but that they may misunderstand their interests, capabilities and behaviour.

The session began with a consideration of simple and recognisable use cases in which major challenges can already be seen (though they will become more complex). IoX components and their complex or hybrid assemblages will and should interact with others, so they must be identified uniquely and discovered with appropriate levels of precision, reliability, and permanence and be capable of enrolment in or separation from IoX systems. The concept of ‘identity’ has some subtlety. For instance, a smart home must be able to recognise and be recognised by new IoT components added to the system on a permanent or temporary basis, accorded the right kinds of access and privileges and tracked or remembered appropriately. These identities enable necessary functions, including the granting of trust. But they need not be unique, durable or universal. Indeed, categorical or shared identities (e.g., type certification) may be more practicable, scalable, flexible, future-proof, secure and robust to, e.g., (hardware, software or data) updates and interconnection or federation to create identifiable hybrid systems. Three subtleties linked to identity that came up in the discussion were security (including but not limited to cybersecurity), privacy (including but not limited to data privacy) and ownership (including protections against identity theft or misuse and, conversely, the use of identity to carry liability or responsibility).

Various identity schemes were discussed, ranging from central registries of semi-permanent discrete identities (along the lines of the DNS model) to purely transactional or temporary mutual authentication and identification schemes. These have advantages and drawbacks ranging from theoretical to practical, including technical, legal, commercial, security and other considerations. No single approach seemed to fit all foreseeable circumstances. In placing these in context, the panel recognised that the same concepts applied to the human beings (and organisations) that create, operate and use the IoX. For example, a person is more important than devices or data attributed to him/her, and human rights and responsibilities (e.g., of association and expression) cannot safely be extended to, say, their smart digital assistants. This cuts two ways; it may not be useful to hold a human

being accountable for what their devices do in response to interactions with other systems, which the 'user' may not even perceive, let alone understand or control. Conversely, the automation of routine functions may result in their receiving less considered and responsible human attention, with unintended, undesirable and possibly irreversible results.

The discussion also considered desirable properties that might provide an ethical framework for IoT governance. Many are familiar, e.g., interoperability, transparency and accountability, robustness, resilience, trustworthiness, user empowerment, privacy and security. They are not IoT-specific but may need to be reinterpreted in that context. For example, IoT devices can harvest a wide range of data almost invisibly, which creates general privacy and security risks and affects global development, e.g., via 'data colonialism' whereby devices originating in and provisioned by the global north can be used to capture data from users in the global south to produce innovations for the benefit of the north and to lock in users in the south in ways that inhibit their techno-societal development.

One desideratum came up in relation to technologies, service provision, use cases, data issues, labelling and certification schemes and legal frameworks, and *scalability*. This is a generic issue, but the panel highlighted aspects that stand out clearly in the IoT context. One is *complexity*; as systems scale quantitatively, their qualitative properties may change and, with them, the appropriate kind of governance. Rules may need to be more general, neutral, principles- or function-based. Alternatively, governance may need to move between the data, device, software, etc., planes as systems interconnect in larger and more diverse ways. Another is *practicability*; effective governance may require limits on scale or interoperability. A further aspect is *Quality of Service* (QoS). The IoT-specific emphasis on low latency can constrain system scale, security or flexibility. Beyond this, QoS considerations may lead to multi-tier systems, which may reduce economic welfare, hinder interoperability or distort innovation. Large-scale systems may also be more susceptible to intentional or accidental compromise; effective access control in large environments may lead to inappropriate inclusions or exclusions. Under *laissez-faire* evolution, IoT systems may reach stable sizes and configurations, but these may not be optimal. Finally, very large systems may be difficult to govern with national or self-regulatory arrangements. For example, identification and certification schemes that identify individual devices or types scale with their number but cannot identify even pairwise interactions (which scale as the square of the number of interacting entities). As scale increases, management overloads, costs increase, and utility and use eventually decline. This, however, depends on the governance architecture; a centralised system (analogous to the cloud) offers economies of scale (or diseconomies) and a natural platform for observing systemic behaviour and emergent threats (if not weak signals). However, it creates additional power asymmetries and vulnerabilities; no one governance architecture will likely fit all cases. The group also mentioned other aspects of scale, such as environmental impact.

Another aspect that ran through the various phases of the discussion was trust and trustworthiness; beyond the customary discussion of e-trust, the panel contrasted high-trust and Zero-trust approaches to the problems of identification and interoperability.

The issue of AI in the IoT comes up often but not in depth. The panel recognised that it complicated the IoT, especially when considering smart devices and the emergent intelligence of connected systems. Foreseeability and explicability were discussed, as was the possibility that data-driven systems might be particularly vulnerable to noisy or biased data.

The panel considered various legal approaches and the 'regulatory game' being played out among countries, industries and civil society groups. Governance competition could spur the development of innovative and effective standards if different approaches can be compared and a suitable global

standard emerges through a kind of 'Brussels Effect'. This seems more promising than a too-rapid imposition of global standards and regulations whose implications cannot be foreseen. However, this result is not guaranteed; we could see damaging fragmentation or a rich diversity of approaches matching different contexts. Research on policy initiatives in 40 countries around the world shows that governments often do not regard modern global open source standards and global good practices with security at the core as "important". It was suggested that governments could lead the way by taking such standards actively on board in their procurement activities. Keeping the discussion going and actively engaging with other DCs guarantees a positive outcome and an increased understanding of good global practices in IoT governance. Three important takeaways:

- *IoT data, especially* AI-enhanced, should be understandable, accessible, interoperable, reusable, up-to-date and clear regarding provenance, quality and potential bias.
- At the level of *devices*, there need to be robust mechanisms for finding, labelling, authenticating and trusting devices (and classes of devices). These should survive retraining, replacement or updating but be removable when necessary for functional, security or privacy reasons. To ensure IoT functionality, trustworthiness and resilience, market information and incentives should be aligned. Labels provide a powerful tool; many countries have developed and adopted IoT trust marks, and the time has come to start working towards their international harmonisation.
- *Functions* are not all confined to single devices, designed in or provided by system integrators; they can also be discovered by end-users or emerge from complex system interactions in cyber-physical systems (CPS) and IoT-enabled services. Governance requires methods for recognising, protecting and controlling these functions and their impacts.

-=O=-